described above). Alternatively, a chip with an embedded microprocessor and other components (such as a digital-signal-processor block) to implement the various algorithms described herein) may be used instead. The Intel Xscale™ Microarchitecture from Intel Corp. (Santa Clara, Calif.) is an example. (See http://developer.intel.com/design/intelxscale/index.htm.)

[0022] The circuit **3**A may be embedded using the chip-on-glass process known in the art. The circuit **3**A may be one or more ASICs.

[0023] **FIGS. 1 and 2** illustrate the touch pad **1** of a payment device, according to one embodiment of the invention. The touch pad **1** may include a conductive flexible membrane **11**, insulated dots **18** and a rigid backer **14**. Between the membrane **11** and the rigid substrate **14**, the touch pad **1** may include the display **37**, control circuitry **3**A and a communications link **16**.

[0024] The display **37** may be one or more LCDs, one or more LEDs of the art or both.

[0025] The link **16** communicatively couples the control circuit **3**A and the display **37**.

[0026] In a process herein termed "keypad obfuscation," Lungaro et al., U.S. patent application Ser. No. 09/588,109, "A Secure, Encrypting PIN Pad," encrypts PIN pad data before the data travels beyond the PIN pad. The touch pad **1** described herein may apply keypad obfuscation to data entered on it. Data such as PIN and account numbers may be obfuscated, as may data for transmission to payment processors, keys for password verification and program validation, etc. The encryption circuit **32** may provide this service.

[0027] The signature-capture circuit **34** enables the device **1** to capture and validate signatures entered via the touch pad **1**.

[0028] For the benefit of a customer transacting business on a device incorporating the touch pad **1**, the encryption circuit **32** may direct the display controller **3**B to display an icon or other predetermined indicator visible to the customer on the display **37**. The encryption circuit **32** may do so when it has determined that data to be entered on the touch pad **1** will be secure. The visible indicator ensures the user that the device **1** is indeed secure for data entry.

[0029] Consider the use of an embodiment of the invention in a personal digital assistant (PDA). The touchpad would be used primarily for data entry (e.g., as a graffiti pad). In such cases, the encryption functions are not used. However, when the user wishes to perform a financial transaction, for example, the security functions are activated.

[0030] A typical transaction may progress as follows: When the user initiates a transaction, the microprocessor **31** initiates the display of, say, a virtual PIN pad on the display **39** by invoking a software routine, say, the Virtual PIN Pad routine (VPPR). Now the VPPR cues the security circuit **32** to initialize the security functions. Among the initializations is the display of the secure icon on the display **37**.

[0031] The VPPR cue to the security circuit **32** may include a binary code. If the security circuit **32** does not recognize the code, it does not display the security icon on the display **37**. If a further level of security is deemed necessary, the original VPPR may have a code generator synchronized with the security circuit **32**. Then the binary coded cue changes each time it is generated.

[0032] Then the user enters PIN data which is directed to the cryptography block **32** for encryption. Thus, information leaving the glass is encrypted.

[0033] A hypothesized hacker seeks to bypass the security block **32** to obtain unencrypted PIN data. Assume, arguendo, that he gains control of the microprocessor **31** and uses software of his design to mimic the actions of the original VPPR. He attempts to cue the microprocessor **32** to display the security icon.

[0034] Since the software in the payment device is compiled, the prospective hacker needs the original source code to identify and transmit the necessary binary code.

[0035] The ersatz VPPR has to generate the valid cue. If the security block **32** does not recognize the code proffered, it will not initiate the display of the security icon. The user recognizes the absence of the security icon and refrains from entering sensitive data (e.g., a PIN). Indeed, the encryption circuit **32** may initiate the disablement of the PDA.

[0036] The device **1** may have a separate visible indicator for each type of data that a customer may enter. For example, a first icon may indicate a device **1** secure for PIN entry, while a second different icon may indicate that the device **1** is secure for signatures. In addition or in the alternative, a single visible indicator may indicate that two or more types of data may be entered securely or that any of multiple types of data may be entered securely.

[0037] A visible security indicator is not part of the main display **39** of a touchscreen incorporating the touch pad **1** but is a separate display **37** under different control than the main display **39**. For example, the main display **39** of a touchscreen is typically under the programmatic control of a processor **31** while the display **37** is under the control of the security circuit **32**.

[0038] Data entered on and encrypted by the touch pad **1** is made available to external processors by means of a communications link from the control circuit **3**A. This may be the "pigtail" of the art.

[0039] The class of devices incorporating a touch pad **1** may include point-of-sale (POS) devices, automated teller machines (ATMs), kiosks, mobile phones, keyboards, internet-protocol phones (Voice Over IP or VoIP), laptops and entertainment consoles. Payment terminals, internet appliances and PDAs have already been mentioned.

[0040] For merchants, a device incorporating a touch pad **1** helps to reduce the cost of a card-payment transaction. The physical security reduces or eliminates the opportunity for fraud. Touch-pad data—including PINs, passwords and signatures—are encrypted at the point-of-entry to ensure the security of this information and decrease the cost of the transaction.

[0041] The invention now being fully described, one of ordinary skill in the art will readily recognize many changes and modifications that can be made thereto without departing from the spirit of the appended claims.